**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF NEW JERSEY**

| | |
|---|---|
| EDWARD MARSHALL and ANN MARIE MARSHALL, on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>GUARDIAN ANALYTICS, INC.; ACTIMIZE INC.; and WEBSTER BANK, NA,<br><br>Defendants. | Case No.: 2:23-cv-02156<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Edward Marshall and Ann Marie Marshall ("Plaintiffs") bring this Class Action Complaint against Defendants Guardian Analytics, Inc. ("Guardian Analytics"), Actimize Inc. ("Actimize"), and Webster Bank, NA ("Webster Bank") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and counsels' investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] for customers of Webster Bank and other banks that utilized the services of Guardian Analytics, including, but not limited to, names, Social Security numbers, and financial account numbers.

2. Defendants' negligence resulted in Plaintiffs and Class Members PII being exposed

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

in a Data Breach ("Data Breach"), causing immediate harm and making them susceptible to identity theft and fraud.

3. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Webster Bank admits that the unencrypted PII obtained by an unauthorized external party included name, Social Security number, and financial account numbers.

4. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

5. The PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, Defendants waited several weeks after the Data Breach occurred to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained as secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiffs and Class Members of that information.

6. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as

a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

8. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

9. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

10. Plaintiff Edward Marshall is a citizen of Connecticut residing in Riverton, Connecticut.

11. Plaintiff Ann Marie Marshall is a citizen of Connecticut residing in Riverton, Connecticut.

12. Defendant Guardian Analytics, Inc. is a Delaware corporation with its principal place of business at 221 River Street, Hoboken, New Jersey, 07030. Guardian Analytics is a wholly-owned subsidiary of Actimize Inc.

13. Defendant Actimize Inc. is a Delaware corporation with its principal place of business at 221 River Street, Hoboken, New Jersey, 07030.

14. Defendant Webster Bank, N.A. is a national bank organized under the laws of Delaware with its principal place of business at 200 Elm Street, Stamford, Connecticut 06902.

15. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

16. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Guardian Analytics to establish minimal diversity.

17. This Court has personal jurisdiction over Defendant Guardian Analytics, Inc. because it operates and is headquartered in this District and conducts substantial business in this District.

18. This Court has personal jurisdiction over Defendant Actimize Inc. because it operates and is headquartered in this District and conducts substantial business in this District.

19. This Court has personal jurisdiction over Defendant Webster Bank, N.A. because it contracts with Defendant Guardian, a company headquartered in this District, and purposely availed itself of the laws of New Jersey.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District.

## IV. FACTUAL ALLEGATIONS

***Background***

21. Guardian Analytics provides "behavioral analytics and machine learning solutions for preventing banking fraud and anti-money laundering."[2]

22. Guardian Analytics privacy policy states[3]:

> The privacy and protection of your personal information is important to us. We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, we cannot guarantee its absolute security.
>
> . . .
>
> We use security software to protect the confidentiality of your personal information. In addition, our business practices are reviewed periodically for compliance with policies and procedures governing the security and confidentiality of our information. Our business practices limit employee access to confidential information, and limit the use and disclosure of such information to authorized persons.

23. Webster Bank is a "leading commercial bank with more than $70 billion in assets."[4]

[2] https://guardiananalytics.com/about-guardian-analytics/
[3] https://guardiananalytics.com/privacy-policy/
[4] https://public.websteronline.com/sites/default/files/documents/4Q22-company-overview.pdf

24. Webster Bank's security statement states[5]:

> Identity theft and fraud can turn your life upside down. We take the privacy and security of your information seriously and our number one goal is to give you peace of mind when it comes to your protection.
>
> . . .
>
> Webster Bank uses enhanced security controls to keep your safety at the top of our list. Learn more about all we do to keep you safe.

25. Plaintiffs and Class Members, who are past and current customers of Webster Bank and other banks, provided and entrusted Webster Bank and other banks with sensitive and confidential information, including their name, Social Security number, and account numbers.

26. Plaintiffs and Class Members relied on Webster Bank and other banks to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

27. Defendants had duties to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

***The Data Breach***

28. On or about April 10, 2023, Webster Bank sent Plaintiffs and Class Members a Notice of Data Breach. Webster Bank informed Plaintiffs and other Class Members that:

> What Happened?
>
> On January 26, 2023, Webster learned that Guardian experienced a data security incident that affected a select number of Webster clients. According to Guardian, upon detecting the incident, Guardian immediately activated their incident response plan and retained a third-party cybersecurity firm to conduct an investigation.
>
> Guardian's investigation revealed that unauthorized third parties

[5] https://public.websteronline.com/security

> accessed certain Guardian systems at various times between November 27, 2022 – January 22, 2023. During that time, the unauthorized third parties acquired files that contained Webster clients' personal information from Guardian's systems and later posted the acquired files on the internet.
>
> What Information Was Involved?
>
> Webster reviewed the data that was taken from Guardian's systems and determined that it contained some of your personal information: your name, Social Security number and financial account number.
>
> What We Are Doing?
>
> Webster has retained third parties to assist with our independent investigation. Additionally, Webster is working with Guardian to ensure they implement enhanced security measures to safeguard their network, systems, and data, including that of Webster's clients. Guardian informed Webster that it has notified law enforcement and is cooperating with their investigation.[6]

29. Webster Bank reported that 191,563 individuals were affected by the Data Breach.[7]

30. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

31. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members.

32. Defendants did not state why they waited nearly three months before notifying Plaintiffs and Class Members that their PII was compromised in the Data Breach.

33. Because Defendants had duties to protect Plaintiffs' and Class Members' PII,

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/a42f73e8-720b-41a2-b892-18181e799668.shtml
[7] *Id.*

Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

34. In the years immediately preceding the Data Breach, Defendants knew or should have known that Guardian Analytics' computer systems were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet.

35. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) unauthorized actors were targeting financial analytics companies such as Guardian Analytics, (ii) unauthorized actors were aggressive in their pursuit of big companies such as Guardian Analytics, (iii) unauthorized actors were leaking corporate information on dark web portals, and (iv) unauthorized actors' tactics included threatening to release stolen data.

36. In light of the information readily available and accessible on the internet before the Data Breach, Webster Bank, having elected to share the unencrypted PII of its customers with Guardian Analytics, and Guardian Analytics, having elected to store that PII and other similar PII from other banks in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendants' types of businesses had cause to be particularly on guard against such an attack.

37. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

38. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to

protect against their publication and misuse in the event of a cyberattack.

***Webster Bank Acquires and Shares with Guardian Analytics the PII of Plaintiffs and Class Members.***

39. As a condition of being a past or current customer of Webster Bank, Webster Bank required that Plaintiffs and Class Members entrust Webster Bank with highly confidential PII.

40. Webster Bank shared the PII of Plaintiffs and Class Members with Guardian Analytics, which stored the PII on its Internet-accessible network.

41. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

42. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

43. To date, Defendants offered Plaintiffs and Class Members only two years of personal information misuse detection and identity protection support through Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

***Securing PII and Preventing Breaches***

44. Defendants could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

45. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is

exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

48. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information***

49. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit

[8] 17 C.F.R. § 248.201 (2013).
[9] *Id*.
[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

50. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

51. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the

---

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).
[12] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).
[13] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2022).

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[15]

55. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

56. The fraudulent activity resulting from the Data Breach may not come to light for years.

57. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2022).

[15] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

> the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

58. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

59. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

60. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in the PII that Defendants stored unencrypted, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

## V. CLASS ALLEGATIONS

62. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

63. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was compromised in the Data Breach.

---

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

64. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

65. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

66. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendants have identified thousands of individuals whose PII was compromised in the Data Breach, and the Class is apparently identifiable within Defendants' records. Webster Bank reported that 191,563 individuals were affected by the Data Breach.[17]

67. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had duties to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

[17] https://apps.web.maine.gov/online/aeviewer/ME/40/a42f73e8-720b-41a2-b892-18181e799668.shtml

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

68. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

69. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

70. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

71. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim,

it would still be economically impractical and impose a burden on the courts.

72. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

73. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

74. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

75. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

76. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the

Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

77. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed legal duties to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached legal duties to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Webster Bank on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Webster Bank breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

**COUNT I**
**NEGLIGENCE**
**(On Behalf of Plaintiffs and the Nationwide Class)**

78. Plaintiffs reallege and incorporate by reference herein all preceding paragraphs as if fully set forth herein.

79. As a condition of being customers of Webster Bank, Plaintiffs and the Nationwide Class were obligated to provide and entrust Defendants with certain PII.

80. Plaintiffs and the Nationwide Class provided and entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

81. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

82. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

83. Defendants had duties to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. These duties include, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendants' possession was adequately secured and protected.

84. Defendants also had duties to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII they were no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

85. Defendants also had duties to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

86. Defendants' duties to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Webster Bank and other banks with their confidential PII, a necessary part of obtaining services from Webster Bank and other banks, and Webster Bank and other banks shared that PII with Guardian Analytics.

87. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

88. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

89. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored in an Internet-accessible environment.

90. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take

the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendants.

91. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

92. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

93. Defendants had and continue to have duties to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

94. Defendants had duties to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

95. Defendants have admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

96. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendants' possession or control.

97. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the

Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

98. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

99. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

100. Defendants breached their duties to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII they were no longer required to retain pursuant to regulations and which Defendants had no reasonable need to maintain in an Internet-accessible environment.

101. Defendants, through their actions and/or omissions, unlawfully breached their duties to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

102. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

103. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate

security measures.

104. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

105. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

106. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so

long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

107. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

## COUNT II
## BREACH OF IMPLIED CONTRACT
## (Against Webster Bank on Behalf of Plaintiffs and the Nationwide Class)

108. Plaintiffs reallege and incorporate by reference herein all preceding paragraphs as if fully set forth herein.

109. In being customers of Webster Bank, Plaintiffs and the Nationwide Class provided and entrusted their PII to Webster Bank.

110. Webster Bank's website confirms that Webster Bank intended to bind itself to protect the PII that Plaintiffs and the Nationwide Class submitted to Webster Bank.

111. Webster Bank required Plaintiffs and the Nationwide Class to provide and entrust their PII as condition of being past and current customers of Webster Bank.

112. As a condition of being past and current customers of Webster Bank, Plaintiffs and the Nationwide Class provided and entrusted their PII. In so doing, Plaintiffs and the Nationwide Class entered into implied contracts with Webster Bank by which Webster Bank agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their PII had been compromised or stolen.

113. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Webster Bank.

114. Webster Bank breached the implied contracts it made with Plaintiffs and the Nationwide Class by (i) failing to encrypt Plaintiffs' and the Nationwide Class's PII before sharing

it with Guardian Analytics and (ii) failing to ensure that Guardian Analytics encrypted the PII while storing it in an Internet-accessible environment, and (iii) failing to ensure that Guardian Analytics otherwise safeguarded and protected the PII.

115. As a direct and proximate result of Webster Bank's above-described breach of implied contract, Plaintiffs and the Nationwide Class have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their sensitive information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

116. As a direct and proximate result of Webster Bank's above-described breach of implied contract, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

## COUNT III
### Declaratory Judgment
### (As to Webster Bank on Behalf of Plaintiffs and the Nationwide Class)

117. Plaintiffs reallege and incorporate by reference herein all preceding paragraphs as if fully set forth herein.

118. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

119. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Webster Bank is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Webster Bank's data security measures remain inadequate. Webster Bank publicly denies these allegations. Furthermore, Plaintiffs and the Nationwide Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Webster Bank has undertaken in response to the Data Breach.

120. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Webster Bank's inadequate security measures, including (i) Webster Bank's failure to encrypt Plaintiffs and the Nationwide Class's PII before sharing it with Guardian Analytics, (ii) Webster Bank's failure to ensure that Guardian Analytics encrypted the PII while storing it in an Internet-accessible environment, (iii) Webster Bank's failure to ensure that Guardian Analytics otherwise safeguarded and protected the PII, and (iv) Webster Bank's failure to ensure that Guardian Analytics deleted any PII it no longer had a reasonable need to maintain.

121. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Webster Bank owes a legal duty to secure the PII of past and current customers of Webster Bank;

b. Webster Bank continues to breach this legal duty by failing to employ reasonable measures to secure the PII; and

c. Webster Bank's ongoing breaches of its legal duties continue to cause harm to Plaintiffs and the Nationwide Class.

122. This Court also should issue corresponding prospective injunctive relief requiring Webster Bank to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Webster Bank to:

a. Encrypt the PII of customers before sharing it with other entities;

b. Ensure that such entities safeguard and protect such PII, including by storing it in encrypted form; and

c. Ensure that such entities delete any such PII they no longer have a reasonable need to maintain.

123. If an injunction is not issued, Plaintiffs and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Guardian Analytics or some other entity with which Webster Bank shares the PII. The risk of another such breach is real, immediate, and substantial. If another breach at Guardian Analytics or another entity with which Webster Bank shares the PII occurs, Plaintiffs and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

124. The hardship to Plaintiffs and the Nationwide Class if an injunction is not issued exceeds the hardship to Webster Bank if an injunction is issued. Plaintiffs and the Nationwide Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Webster Bank of complying with an injunction by employing reasonable prospective data

security measures is relatively minimal, and Webster Bank has a pre-existing legal obligation to employ such measures.

125. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing or mitigating another data breach at Guardian Analytics or another entity with which Webster Bank shares the PII, thus eliminating or mitigating the additional injuries that would result to Plaintiffs and the Nationwide Class and others whose confidential information would be further compromised.

**COUNT IV**
**Declaratory Judgment**
**(As to Guardian Analytics on Behalf of Plaintiffs and the Nationwide Class)**

126. Plaintiffs reallege and incorporate by reference herein all preceding paragraphs as if fully set forth herein.

127. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

128. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Guardian Analytics is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Guardian Analytics' data security measures remain inadequate. Guardian Analytics publicly denies these allegations. Furthermore, Plaintiffs and the Nationwide Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is

unknown what specific measures and changes Guardian Analytics has undertaken in response to the Data Breach.

129. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Guardian Analytics' inadequate security measures, including (i) Guardian Analytics' failure to encrypt Plaintiffs and the Nationwide Class's PII while storing it in an Internet-accessible environment, (ii) Guardian Analytics' failure otherwise safeguard and protect the PII, (iii) Guardian Analytics' failure to delete any PII it no longer had a reasonable need to maintain.

130. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Guardian Analytics owes a legal duty to secure the PII of past and current customers of Webster Bank;

b. Guardian Analytics continues to breach this legal duty by failing to employ reasonable measures to secure the PII; and

c. Guardian Analytics' ongoing breaches of its legal duties continue to cause harm to Plaintiffs and the Nationwide Class.

131. This Court also should issue corresponding prospective injunctive relief requiring Guardian Analytics to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Guardian Analytics to:

a. Encrypt the PII of Webster Bank's customers;

b. Otherwise safeguard and protect such PII; and

c. Delete any such PII it no longer has a reasonable need to maintain.

132. If an injunction is not issued, Plaintiffs and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Guardian Analytics. The risk of another such breach is real, immediate, and substantial. If another breach at Guardian Analytics occurs, Plaintiffs and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

133. The hardship to Plaintiffs and the Nationwide Class if an injunction is not issued exceeds the hardship to Guardian Analytics if an injunction is issued. Plaintiffs and the Nationwide Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Guardian Analytics of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Guardian Analytics has a pre-existing legal obligation to employ such measures.

134. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing or mitigating another data breach at Guardian Analytics, thus eliminating or mitigating the additional injuries that would result to Plaintiffs and the Nationwide Class and others whose confidential information would be further compromised.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiffs and their counsel to represent such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Guardian Analytics network is compromised, hackers cannot gain access to other portions of Guardian Analytics' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective

employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Guardian Analytics' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Guardian Analytics' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand that this matter be tried before a jury.

Date: April 18, 2023

Respectfully Submitted,

*/s/ David C. Magagna*

Charles E. Schaffer*
David C. Magagna
Nicholas J. Elia*
**LEVIN SEDRAN & BERMAN**
510 Walnut Street, Suite 500
Philadelphia, PA 19106
(215) 592-1500
cschaffer@lfsblaw.com
dmagagna@lfsblaw.com
nelia@lfsblaw.com

Jeffrey S. Goldenberg*
**GOLDENBERG SCHNEIDER, LPA**
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
(513) 345-8291
jgoldenberg@gs-legal.com

*Attorneys for Plaintiffs and the Proposed Class*

**pro hac vice applications forthcoming*